

Stephen M. Orlofsky
BLANK ROME, LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540
(609) 750-7700

Bruce P. Keller
Jeremy Feigelson
(*Pro Hac Vice* admission pending)
Kristin Lieske Bryan
(*Pro Hac Vice* admission pending)
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, NY 10022
(212) 909-6000

Attorneys for Defendant Viacom Inc.

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

IN RE: NICKELODEON
CONSUMER
PRIVACY LITIGATION

MDL No. 2443

Docket No. 2:12-cv-07829
(SRC)(CLW)

This Document Relates To: ALL
CASES

ECF Case

**REPLY MEMORANDUM OF LAW IN
SUPPORT OF DEFENDANT
VIACOM INC.'S MOTION TO DISMISS**

Oral Argument Requested

TABLE OF CONTENTS

PRELIMINARY STATEMENT	1
ARGUMENT	2
I. Plaintiffs Do Not Have Standing.	2
II. Plaintiffs Fail to State a Claim Under Federal Law.	7
A. Plaintiffs Fail to State a Claim Under VPPA.	7
B. Plaintiffs Fail to State a Claim Under ECPA.	13
1. The Statute’s One-Party Consent Structure Requires Dismissal of the ECPA Claim.	13
2. Viacom Did Not Disclose the “Contents” of Plaintiffs’ Communications.	15
3. Viacom Has No Liability Under ECPA for Google’s Conduct.	19
III. Plaintiffs’ State Law Claims Should Be Dismissed.	20
A. COPPA Preempts Plaintiffs’ State Law Claims.	20
B. Plaintiffs Fail to State a Claim Under State Law.	21
1. Plaintiffs Have Not Stated a Claim Under the California Invasion of Privacy Act.	21
2. Plaintiffs Have Not Stated a Claim Under the New Jersey Computer Related Offenses Act.	22
3. Plaintiffs Have Not Stated a Claim for Intrusion Upon Seclusion or Unjust Enrichment.	23
CONCLUSION	25

TABLE OF AUTHORITIES

Cases

<i>Alston v. Countrywide Fin. Corp.</i> , 585 F.3d 753 (3d Cir. 2009)	3
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	22
<i>Berk v. JP-Morgan Chase Bank, N.A.</i> , No. 11-2715, 2011 WL 6210674 (E.D. Pa. Dec. 13, 2011)	14, 15
<i>Caro v. Weintraub</i> , 618 F.3d 94 (2d Cir. 2010)	14, 15
<i>Chance v. Ave. A., Inc.</i> , 165 F. Supp. 2d 1153 (W.D. Wash. 2001)	14, 15
<i>Cohen v. Facebook, Inc.</i> , Case No. BC444482 (Cal. Super., minute order Sept. 30, 2011)	21
<i>Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz</i> , 891 F. Supp. 2d 13 (D.D.C. 2012)	20
<i>Danvers Motor Co. v. Ford Motor Co.</i> , 432 F.3d 286 (3d Cir. 2005)	3
<i>Del Vecchio v. Amazon.com Inc.</i> , No. C11-366, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011)	4
<i>Dirkes v. Borough of Runnemede</i> , 936 F.Supp. 235 (D.N.J. 1996)	10
<i>Doe v. Chao</i> , 540 U.S. 614 (2004)	7
<i>Fairfield v. Am. Photocopy Equip. Co.</i> , 138 Cal. App. 2d 82 (Cal. Dist. Ct. App. 1955)	6

<i>Fowler v. S. Bell Tel. & Tel. Co.,</i> 343 F.2d 150 (5th Cir. 1965)	6
<i>G.D. v. Kenny,</i> 205 N.J. 275 (2011)	25
<i>In re § 2703(d) Order,</i> 787 F. Supp. 2d 430 (E.D. Va. 2011)	16
<i>In re DoubleClick Inc. Privacy Litig.,</i> 154 F. Supp. 2d 497 (S.D.N.Y. 2001)	13, 15, 25
<i>In re Google, Inc. Privacy Policy Litig.,</i> No. C-12-01382, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013)	5
<i>In re Hulu Privacy Litig.,</i> No. C 11-03764, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012)	9
<i>In re Hulu,</i> No. C11-03764, 2013 WL 6773794 (N.D. Cal. Dec. 20, 2013)	10
<i>In re: Google, Inc. Cookie Placement Consumer Privacy Litig.,</i> No. 12-2358-SLR, 2013 WL 5582866 (D. Del. Oct. 9, 2013)	16, 22, 25
<i>Kirch v. Embarq Mgmt. Co.,</i> 702 F.3d 1245 (10th Cir. 2012)	19
<i>L.C. v. Cent. Pa. Youth Ballet,</i> No. 1:09-cv-2076, 2010 WL 2650640 (M.D. Pa. July 2, 2010)	14
<i>LaCourt v. Specific Media, Inc.,</i> No. SACV 10-1256, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011)	4, 5
<i>Lonegan v. Hasty,</i> 436 F. Supp. 2d 419 (E.D.N.Y. 2006)	19
<i>Lujan v. Defenders of Wildlife,</i> 504 U.S. 555 (1992)	3, 4
<i>McDaniel v. Atlanta Coca-Cola Bottling Co.,</i> 2 S.E. 2d 810 (Ga. 1939)	6

<i>Nat’l Amusements, Inc. v. N.J. Turnpike Auth.</i> , 261 N.J. Super. 468 (N.J. Super. 1992).....	24
<i>Pearson v. Dodd</i> , 410 F.2d 701 (D.C. Cir. 1969).....	6
<i>Peavy v. WFAA-TV, Inc.</i> , 221 F.3d 158 (5th Cir. 2000)	19, 20
<i>Pennsylvania ex rel. Zimmerman v. PepsiCo, Inc.</i> , 836 F.2d 173 (3rd Cir. 1988).....	9
<i>Pichler v. UNITE</i> , 542 F.3d 380 (3d Cir. 2008)	9
<i>PNY Technologies, Inc. v. Salhi</i> , No. 2:12-cv-04916, 2013 WL 4039030 (D.N.J. Aug. 5, 2013)	23
<i>Rhodes v. Graham</i> , 37 S.W.2d 46 (Ky. 1931).....	6
<i>Shefts v. Petrakis</i> , 954 F. Supp. 2d 769 (C.D. Ill. 2013).....	20
<i>Sterk v. Best Buy Stores, L.P.</i> , No. 11 C 1894, 2012 WL 5197901 (N.D. Ill. Oct. 17, 2012)	6, 7
<i>United States v. Allen</i> , 53 M.J. 402 (C.A.A.F. 2000).....	22
<i>United States v. Dale</i> , 991 F.2d 819 (D.C. Cir. 1993).....	15
<i>United States v. Tarantino</i> , No. 08–CR–0655, 2012 WL 5430865 (E.D.N.Y. Nov. 7, 2012).....	15
<i>Viacom Int’l Inc. v. Youtube Inc.</i> , 253 F.R.D. 256 (S.D.N.Y. 2008).....	11
<i>Vill. of Bloomingdale v. CDG Enterprises, Inc.</i> , 196 Ill. 2d 484 (2001)	24

<i>Warth v. Seldin</i> , 422 U.S. 490 (1975)	4
---	---

<i>Yunker v. Pandora Media, Inc.</i> , No. 11-cv-03113, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013).....	18
---	----

Statutes

15 U.S.C. § 6501	10, 11
15 U.S.C. § 6502	20
18 U.S.C. § 2520	17
18 U.S.C. § 2710	7, 8, 10, 13
18 U.S.C. § 2721	9
18 U.S.C. § 3121	17
18 U.S.C. § 3123	17
N.J. Stat. 2A:38A-3	23

Other Authorities

15 A.L.R. Fed. 2d 537 (2006)	17
No. 1301, A1301, ch. 184, 1984 N.J. Laws 1 (1984)	23
S. Rep. No. 100-599, <i>reprinted in</i> 1988 U.S.C.C.A.N. 4342-1	8

PRELIMINARY STATEMENT

Stripped of rhetoric and a raft of assertions pleaded nowhere in the Complaint, Plaintiffs' brief asserts only that the Viacom websites at issue use cookies – a commonplace technology that repeatedly has been held lawful. There are only two purported distinctions between this Complaint and the many others, also objecting to cookies, that have been dismissed at the pleading stage.

First, this Complaint alleges that Plaintiffs are children. Second, it hypothesizes that the anonymous information collected through cookies *might* someday be manipulated in ways that could result in the disclosure of Plaintiffs' actual identities. Memorandum of Law in Support of Defendant Viacom Inc.'s Motion to Dismiss ("Viacom Br.") 12–18.

These are distinctions without a difference. Plaintiffs' status as children does not change the governing legal standard. No actual disclosure of personal information or any economic injury is alleged to have occurred. Regardless of Plaintiffs' age, they have alleged no concrete injury, which means they have no standing. Their failure to allege the actual disclosure of information that personally identifies them also means they do not state a federal claim either under VPPA, *id.* 18–24, or, given Viacom's one-party consent to the use of cookies, under ECPA, *id.* 25–31. The ECPA claim fails for the additional reason that Plaintiffs plead neither any interception of the contents of their communications

nor any tortious purpose on Viacom's part. *Id.* 25–31. Nor does the Complaint provide any basis for proceeding under state law, in light of the doctrines of supplemental jurisdiction and preemption, *id.* 32–33, and the failure to allege any state-law violations, *id.* 34–38.

Like the Complaint itself, Plaintiffs' opposition relies on generalized overstatements and on policy arguments about children and privacy. The actual allegations of the Complaint, however, simply do not describe any cognizable injury-in-fact or any violation of law. The Court should dismiss the Complaint with prejudice.

ARGUMENT

I. Plaintiffs Do Not Have Standing.

The information collected through Viacom's cookies, and shared with Google through automated systems, is entirely anonymized. *See* Complaint ("Compl.") ¶¶ 60–65 (speculating that companies may take steps to identify or deanonymize Internet users); Plaintiffs' Omnibus Opposition to the Motions to Dismiss from Defendants Viacom and Google ("Pl. Br.") 4–8 (asserting only that Viacom used cookies to track Plaintiffs' anonymous activities on Viacom's websites). Plaintiffs pin their case on the speculation that, at some time in the future, someone hypothetically might be able to connect the dots between that anonymous information and their real-world identities.

That contention is constitutionally insufficient for standing, because it does not satisfy the requirement that injury-in-fact be “concrete and particularized” and “actual or imminent,” as opposed to “conjectural or hypothetical” allegations that, at some point, Plaintiffs’ personally identifiable information or contents of their communications might be disclosed. *See Danvers Motor Co. v. Ford Motor Co.*, 432 F.3d 286, 290–91 (3d Cir. 2005) (Alito, J.) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992)); *Viacom Br.* 12–18.

Plaintiffs point to nothing to distinguish themselves from all other users of the Internet – of any age – any one of whom might someday be subjected to the hypothetical de-anonymization of data collected through cookies. Plaintiffs’ own authority, *Alston v. Countrywide Fin. Corp.*, 585 F.3d 753 (3d Cir. 2009), *Pl. Br.* at 9–10, confirms that this failure to identify an injury plaintiffs themselves have suffered, in a way that is distinct from the general population, is a failure to plead Article III injury-in-fact.

The *Alston* plaintiffs pled they personally had been victimized by mortgage-lending kickback schemes. That was “a particularized injury” under the Real Estate Settlement Procedures Act of 1974, *Alston*, 585 F.3d at 763, as contrasted with a case “in which plaintiffs press ‘a “generalized grievance” shared in substantially equal measure by all or a large class of citizens,’” and therefore lack standing, *id.* (quoting *Warth v. Seldin*, 422 U.S. 490, 499 (1975)).

This is that generalized case. Plaintiffs object to the ordinary operation of the Internet as millions experience it every day. Pl. Br. 3 (“[F]irst-party cookies [like Viacom’s] may indeed be essential for how the Internet functions . . .”). Even if Plaintiffs state their objection in terms that mirror the elements of a federal statutory claim, they must, under Article III, plead a **concrete** injury (1) that they **actually suffered** or will imminently suffer and (2) that is more than a “generalized grievance” shared by substantially all. *See Lujan*, 504 U.S. at 560, 575.

Plaintiffs’ allegations of injury are even weaker than in other cases where plaintiffs were held to lack standing despite making the same argument advanced here – *i.e.*, that they did not consent to the defendants’ use of cookies because the cookies were transferred automatically to their computers. In those cases, there were specific allegations that personal data actually had been misused. *See Del Vecchio v. Amazon.com Inc.*, No. C11-366, 2011 WL 6325910, at *1 (W.D. Wash. Dec. 1, 2011); *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256, 2011 WL 1661532, at *1 (C.D. Cal. Apr. 28, 2011). That still was not enough, and here that allegation is not even made. Instead, the alleged injury is purely speculative. By their own allegations, Plaintiffs’ personal information has yet to actually be disclosed and has yet to lose whatever theoretical value it has (*i.e.*, there is no claim that Defendants’ efforts have taken money out of Plaintiffs’ pockets). Compl. ¶¶ 49–59.

Absent allegations that such injuries either already occurred or are imminent, the use of cookies by Viacom does not establish standing. *See In re Google, Inc. Privacy Policy Litig.*, No. C-12-01382, 2013 WL 6248499, at *2–3, 5 (N.D. Cal. Dec. 3, 2013) (declining to find Article III standing absent “an allegation that [defendant’s] profiteering deprived Plaintiffs’ [*sic*] of economic value”). Plaintiffs’ status as minors does not change the standing analysis.

Plaintiffs’ suggestion that they “adequately and specifically pled economic damages as a result of [the Defendants’ alleged] privacy intrusions,” Pl. Br. 13 (citing Compl. ¶¶ 49–59), exemplifies what permeates their brief: exaggeration of the facts actually alleged. Paragraphs 49 through 59 of the Complaint do not contain a single allegation about Plaintiffs themselves. Instead, they cite miscellaneous law review articles, newspaper articles and psychological studies about possible disclosures of personal information in the abstract. It is the antithesis of “specific” to plead damages based on academic notions of how to quantify injuries that Plaintiffs do not allege they themselves have suffered. *Id.*; *see also LaCourt*, 2011 WL 1661532, at *3–5 (finding no standing absent a “particularized example” of actual injury). Because Plaintiffs fail to plead that

they have suffered concrete, particularized and non-speculative harm, their entire Complaint should be dismissed on that basis alone.¹

Plaintiffs' references to a generalized theory of invasion of privacy, Pl. Br. 11–12, fail to cure this defect. The state-law cases on which they rely involved specific allegations of emotional injuries and/or actual damages – allegations of a kind that are entirely lacking here. *See McDaniel v. Atlanta Coca-Cola Bottling Co.*, 2 S.E. 2d 810, 812 (Ga. 1939) (damages of \$100,000 for mental pain and distress); *Rhodes v. Graham*, 37 S.W.2d 46, 47 (Ky. 1931) (damages of \$5,000 for mental anguish); *Fairfield v. Am. Photocopy Equip. Co.*, 138 Cal. App. 2d 82, 86–87 (Cal. Dist. Ct. App. 1955) (pleading harm from mental anguish). In the two federal cases Plaintiffs cite, the courts were not concerned with determining whether there was cognizable injury because plaintiffs' standing was not challenged. *See Pearson v. Dodd*, 410 F.2d 701 (D.C. Cir. 1969); *Fowler v. S. Bell Tel. & Tel. Co.*, 343 F.2d 150 (5th Cir. 1965). The unsupported assertion of an injury from an invasion of privacy is insufficient to satisfy Article III's injury-in-fact requirement.

¹ Standing is so plainly absent in these circumstances that this Court need not reach the issue of the scope of Congress' authority to define harm sufficient for Article III standing. As noted in Viacom's opening brief, to the extent the Court opts to address that issue, it should join *Sterk v. Best Buy Stores, L.P.*, No. 11 C 1894, 2012 WL 5197901, at *5 (N.D. Ill. Oct. 17, 2012) in holding that "a [VPPA] plaintiff must plead an injury beyond a statutory violation to meet the standing requirement of Article III." Viacom Br. 21 n. 5.

Plaintiffs have not alleged that Viacom disclosed the real-world identity of any Plaintiff (much less did so in conjunction with the other required elements of a statutory violation) or otherwise caused them any real-world harm. That is fatal to their assertion of standing. *See Sterk*, 2012 WL 5197901, at *5–6 (dismissing VPPA claim in part for failure to plead an Article III injury – *i.e.*, that plaintiff was unable “to sell his *own* information for as much value” (emphasis in original) (citing *Doe v. Chao*, 540 U.S. 614, 621, 627 (2004) (no damages under Privacy Act absent real-world injury))). All the claims in the Complaint should be dismissed for failure to plead an injury sufficient to satisfy Article III.

II. Plaintiffs Fail to State a Claim Under Federal Law.

A. Plaintiffs Fail to State a Claim Under VPPA.

The VPPA claim fails because VPPA prohibits only the disclosure of “information which [(1)] *identifies a person* [(2)] as having requested or obtained *specific video materials* or services from [(3)] a *video tape service provider*.” 18 U.S.C. § 2710(a)(3) (emphasis added); Viacom Br. 18–24. Plaintiffs plead no facts that meet any of those three elements.

On the issue of whether any of them was “identifie[d]” as a “person,” Plaintiffs rely on the policy argument that anonymized data should be deemed to personally identify them even though, on its face, it does not. *See* Compl. ¶¶ 60–65. The data alleged to be at issue does not include, for example, real names,

email addresses, physical addresses, telephone numbers or any other real-world identifying details. Compl. ¶¶ 81, 85–89, 93, 97–99 (alleging the purported disclosures to include profile name, “Rugrat” code name, URL of show landing page, IP address, and technical computer details). That is not enough under either the plain language (“identifies a *person*”) or the legislative history of VPPA. 18 U.S.C. § 2710(a)(3) (emphasis added); S. Rep. No. 100-599, at 5, *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-5 (“Senate Report”).

VPPA was passed in the wake of a video store’s disclosure of Judge Robert Bork’s video rental history to a reporter – *i.e.*, the public release of specific video titles rented by an actually identified, personally named individual. Senate Report, 1988 U.S.C.C.A.N. at 4342-5; Viacom Br. 18–20. That background confirms that the statutory term “person” means a specific individual, recognizable in the real world, and not anonymized “username, sex, age, type of computer, and exact location.” Pl. Br. 20.

The prospect that someone, someday, somewhere could connect the dots between that anonymized data and particular Plaintiffs is not a disclosure covered by the statute. That has not occurred as Plaintiffs’ actual allegations make clear.

- For example, Plaintiffs argue that Viacom disclosed the “sex” and “age” of users to Google – details that were contained only within Viacom’s “Rugrat” code. Pl. Br. 6 (citing Compl. ¶¶ 86–97); *see also* Compl. ¶ 99. Nowhere in

the Complaint, however, do Plaintiffs allege that Google could decrypt or understand the “Rugrat” code that allegedly contained their sex and age.

The statement must therefore be disregarded. *See Pennsylvania ex rel.*

Zimmerman v. PepsiCo, Inc., 836 F.2d 173, 181 (3rd Cir. 1988) (“[I]t is axiomatic that the complaint may not be amended by the briefs in opposition to a motion to dismiss.”).

- None of the other data that Viacom allegedly disclosed either expressly identified a particular person or actually enables the connecting of the dots today. Compl. ¶81. That makes the allegations here very different from *In re Hulu Privacy Litig.*, No. C 11-03764, 2012 WL 3282960, at *2 (N.D. Cal. Aug. 10, 2012), which involved public disclosure of data linked to Facebook IDs – information readily connected to plaintiffs’ real-world identities.
- The Complaint fails even to allege that Viacom had the internal capability of identifying Plaintiffs by name or other real-world details, let alone that Viacom disclosed information that would have allowed others to do so. Compl. ¶¶ 85–93.

Pichler v. UNITE, 542 F.3d 380, 391–92 (3d Cir. 2008), arising under the similar provisions of the Driver’s Privacy Protection Act of 1994 (“DPPA”), 18 U.S.C. § 2721 *et seq.*, confirms that individuals who are not literally identified by the disclosed information cannot state a VPPA claim. Viacom Br. 21–22. DPPA

protects “information that identifies an individual,” as does VPPA. *Compare* 18 U.S.C. § 2725(3), *with* 18 U.S.C. § 2710(a)(3). Plaintiffs attempt to distinguish *Pichler* by citing to another *Hulu* decision, *In re Hulu*, No. C11-03764, 2013 WL 6773794, at *7 (N.D. Cal. Dec. 20, 2013), but the court there expressly stated that “[t]he DPPA and VPPA sections prohibiting disclosure of personal information are similar” and, as noted, the requisite identifying details in *Hulu* were in plain public view. 2013 WL 6773794 at *7.

Dirkes v. Borough of Runnemede, 936 F.Supp. 235 (D.N.J. 1996), which Plaintiffs also cite, underscores the absence of any disclosures of identifying data in this Complaint. *Dirkes* involved the release of specific movie titles explicitly linked to the real names of the people who rented them. *Id.* at 236 (describing disclosure of “the names and rental dates of certain pornographic videotapes previously rented by Plaintiff Dirkes and his wife, co-plaintiff Marie Dirkes”). Nowhere in the *Dirkes* decision did the court suggest the concept of personal information under VPPA should be read any more broadly.

Plaintiffs’ reliance on the FTC’s rulemaking under the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. § 6501 *et seq.*, is likewise misplaced. The COPPA Rule, by its terms, does not apply to VPPA. Congress expressly permitted the FTC to expand upon COPPA’s statutory definition of personally identifiable information, 15 U.S.C. § 6501(8)(F), but gave no such

authority to the FTC or any other agency under VPPA. Moreover, in discussing the COPPA Rule, Plaintiffs again engage in overstatement: they cite to four of the FTC’s definitions of personally identifiable information, including “online contact information” and “persistent identifier[s]” enabling identifications across multiple websites, but they do not actually allege collection or sharing of any of these forms of personally identifiable information by Viacom. *See* Compl. ¶¶ 85–90 (no allegation that users provide contact information, only birthdate, gender, and a “profile name”), ¶¶ 90–91 (no allegation that users are given a persistent identifier enabling identifications across different websites). Plaintiffs’ overstatement appears to be an attempt to invite this Court to reach the conclusion that Viacom has somehow violated COPPA – a conclusion Plaintiffs nowhere expressly assert because Viacom has always complied with COPPA.

Plaintiffs stretch even further when they reference a press release issued in connection with a discovery stipulation in the unrelated case of *Viacom Int’l Inc. v. Youtube Inc.* Pl. Br. 19. The *YouTube* litigation was a copyright case. It does not implicate VPPA at all. Viacom never argued or conceded there that usernames and persistent identifiers constitute personally identifiable information, nor did the court so find. *See Viacom Int’l Inc. v. Youtube Inc.*, 253 F.R.D. 256, 262 (S.D.N.Y. 2008) (granting Viacom’s discovery request, noting that “the login ID is an *anonymous pseudonym* that users create for themselves when they sign up with

YouTube, which *without more cannot identify specific individuals*” and “[t]he reality is though that in most cases, *an IP address without additional information cannot [identify you].*” (internal quotations omitted) (emphasis added)). *YouTube* has absolutely no relevance here, other than to underscore that, because the Complaint lacks adequate allegations, Plaintiffs’ opposition relies heavily (and incorrectly) on sources far beyond what they actually pled.

As to the second element of a VPPA claim, the Complaint fails because it does not allege the disclosure of “specific video materials.” Viacom Br. 24. Plaintiffs tacitly admit this by, again, going far outside their pleading – describing a degree of specificity purportedly contained in URLs, Pl. Br. 31–32, that appears nowhere in the Complaint. Although Plaintiffs point to three places in the Complaint where they purportedly allege that Viacom disclosed with particularity the videos that Plaintiffs viewed, Pl. Br. 20 n.14 (citing Compl. ¶¶ 70–78, 81–97, 122–124), none of these paragraphs actually states Viacom disclosed such specific information to Google.

As to the third and last VPPA element, Viacom also is not a “video tape services provider” in the business of “rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials” under VPPA, because streaming videos (which Viacom provides on Nick.com and NickJr.com) and interactive games (which is all that is available on NeoPets.com) do not fit within the statutory

definition of “similar audio visual materials” according to the Congress that passed VPPA. 18 U.S.C. § 2710(a)(4); *see* S. Rep. No. 100-599, at 10 (identifying “similar” materials in a list comprised exclusively of *physical* media).

B. Plaintiffs Fail to State a Claim Under ECPA.

1. The Statute’s One-Party Consent Structure Requires Dismissal of the ECPA Claim.

ECPA could not be clearer: only one party needs to consent in order to take a disclosure of contents of communications outside of the statute. Viacom consented to the use of cookies alleged here. That brings this case squarely within the longstanding rule of *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), that the use of cookies with one-party consent does not violate ECPA. Viacom Br. 25–27. Plaintiffs’ respond with the irrelevant argument that “a minor’s ability to contract and consent to an agreement has never been treated in the same way as an adult.” Pl. Br. 29. Contracts require two-party consent; ECPA does not.

Plaintiffs try to invoke the “criminal or tortious act” exception to ECPA’s one-party consent regime. 18 U.S.C. § 2511(2)(d); *see DoubleClick*, 154 F. Supp. 2d at 518–19. They essentially concede, however, the exception is inapplicable by arguing Viacom’s conduct was done “for [its] own pecuniary gain” – not for the purpose of committing any tort. Pl. Br. 2; *see Chance v. Ave. A., Inc.*, 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001) (ECPA “liability would only be

possible if the tortious purpose were the *primary motivation or determinative factor*” behind the defendant’s actions and it is “simply implausible that the entire business plan of one of the country’s largest Internet media companies would be primarily motivated by a tortious or criminal purpose” (emphasis added) (internal quotations and modifications omitted)).

The assertion that an “allegation of intrusion upon seclusion is sufficient to invoke the tort/crime exception,” Pl. Br. 29, is entirely circular. Even were there a clear allegation of intrusion (and there is not, *see infra* Part III.B.3), that would “not create liability under the Federal Wiretap Act [a/k/a ECPA] because it fails to satisfy the independent tortious intent requirement.” *Berk v. JP-Morgan Chase Bank, N.A.*, No. 11-2715, 2011 WL 6210674, at *3 (E.D. Pa. Dec. 13, 2011); *see also Caro v. Weintraub*, 618 F.3d 94, 101 (2d Cir. 2010) (holding that plaintiff’s intrusion upon seclusion claim “occurs through the act of interception itself” and “cannot satisfy the Wiretap Act’s requirement of a separate and independent tortious intent”).

Plaintiffs have, however, found one case stating that a violation of ECPA, without more, satisfies the exception. It stands alone and is based on egregious facts that could not be more dissimilar. Pl. Br. 43. In *L.C. v. Cent. Pa. Youth Ballet*, No. 1:09-cv-2076, 2010 WL 2650640, at *2 (M.D. Pa. July 2, 2010), the plaintiff, a minor, was sexually assaulted by another student at a ballet school. A

school employee secretly taped the plaintiff recounting the assault and distributed the tape to others, including the parents of the perpetrator. *Id.* On these facts, without citation to anything except ECPA's text, the court held that the defendant's alleged violation of ECPA in and of itself satisfied the "criminal or tortious act" exception. *Id.* at *2–3. No other court agrees with *L.C.*'s reading of the statute, leaving it to stand only for the familiar proposition that hard facts make bad law. *See Berk*, 2011 WL 6210674, at *3 ("Courts have interpreted [the ECPA] to require that the 'interceptor intend to commit a crime or tort independent of the act of recording itself.'" (quoting *Caro*, 618 F.3d at 100)). The exception in Section 2511(2)(d) is to be construed narrowly, and applied only when the defendant had an independent tortious or criminal purpose beyond the interception itself. *See Caro*, 618 F.3d at 100–01; *United States v. Dale*, 991 F.2d 819, 841–42 (D.C. Cir. 1993); *United States v. Tarantino*, No. 08–CR–0655, 2012 WL 5430865, at *10 (E.D.N.Y. Nov. 7, 2012); *Berk*, 2011 WL 6210674, at *3; *DoubleClick*, 154 F. Supp. 2d at 514–15; *Chance*, 165 F. Supp. 2d at 1162–63. This Court should follow those well-reasoned decisions, not the result-driven approach of *L.C.*

2. Viacom Did Not Disclose the "Contents" of Plaintiffs' Communications.

Viacom's opening brief established that it did not disclose to Google any "contents" of Plaintiffs' communications as would be required to state a claim under ECPA. *See Viacom Br.* 29–30; *In re: Google, Inc. Cookie Placement*

Consumer Privacy Litig. (“*Google Cookie*”), No. 12-2358-SLR, 2013 WL 5582866, at *4–5 (D. Del. Oct. 9, 2013), *appeal docketed*, No. 13-4300 (3rd Cir. Feb. 5, 2014). The contents of a communication are the substance of what the “*user* intended to communicate.” *Id.* at *4 (emphasis added). The URLs at issue here, even if they include the name of a television episode in their text, remain nothing more than character strings generated by Viacom. They demonstrate the user’s intent to connect to a webpage – just as the record of someone dialing a phone number demonstrates only the number called and a desire to connect to the person on the other end. *See Google Cookie*, 2013 WL 5582866, at *4–5 (“contents” include “the spoken words of a telephone call,” but not a “telephone or instrument number” (citing *In re § 2703(d) Order*, 787 F. Supp. 2d 430, 435–36 (E.D. Va. 2011))).

Plaintiffs again reach beyond their Complaint and causes of action to rulings from non-ECPA contexts, including the Pen Register Act, where different privacy concerns are at play. Pl. Br. 30 & n.19. This underscores the extent to which the claims they plead have no basis in the laws they actually claim were violated. The Pen Register Act regulates telephone and cellular communications in addition to Internet communications. 18 U.S.C. §§ 3121–27. It protects identified individuals who are being investigated for criminal conduct. *See* 15 A.L.R. Fed. 2d 537

(2006) (describing the Pen Register Act as a law enforcement tool). All orders issued under the Pen Register Act must specify both

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; [*and*]

(B) the identity, if known, of the person who is the subject of the criminal investigation[.]

18 U.S.C. § 3123(b)(1). By contrast, the civil provisions of the ECPA apply to all wire communications of all persons and allow for one-party consent to intercept communications. 18 U.S.C. § 2520(a). For these reasons, the more rigorous requirements of the Pen Register Act, reflected in the decisions Plaintiffs cite, are off point.

Plaintiffs again stretch beyond their actual allegations when they suggest that Viacom's cookies *intercepted* contents in the form of Plaintiffs' age and gender. Pl. Br. 35. The specific allegations of the Complaint actually are that Viacom disclosed a *code name*, which Viacom alone understood to have meaning about a child's age and gender. *Compare* Compl. ¶ 81, *with* Compl. ¶¶ 87–88, 93, 98. Nowhere do Plaintiffs allege that Viacom decrypted the code for Google, which would have been necessary for the sharing of the code to amount to a sharing of their age and gender.

Plaintiffs also rely on one case – which carefully limited its novel holding to the specific facts before it – to argue that age and gender possibly could be

“contents.” Pl. Br. 35 (citing *Yunker v. Pandora Media, Inc.*, No. 11-cv-03113, 2013 WL 1282980, at *6 (N.D. Cal. Mar. 26, 2013)). In *Yunker*, the Court acknowledged cases holding, in other circumstances, that IP addresses, geolocation, telephone call duration and time, and other similar information about a communication were not contents. *Id.* at *6–7. The plaintiff, however, had specifically alleged a breach of Pandora’s privacy policy, that the policy covered information like demographics and location, and that he specifically intended to communicate that particular information to Pandora – making it “contents” in that context (at least for pleading purposes). *Id.* at *1, 7. That is why the *Yunker* Court specifically said “based on the allegations *in this case*, the Court does not find [the] argument [that zip code, gender, or birthday are not contents] persuasive.” *Id.* at *6 (emphasis in original). Plaintiffs do not and cannot make such a claim here because they do not allege they intended to communicate similar contents to Viacom or that Viacom violated its privacy policy in any way.² Additionally, based on Plaintiffs’ allegations, any information that was acquired by Google was sent directly to Google by Plaintiffs’ browsers, and was therefore not disclosed by Viacom. Compl. ¶¶ 24–31, 39–41, 43–44, 78, 177.

² *Yunker* is significant only in that it is yet another case holding that the possibility that personally identifiable information might be disclosed or stolen in the future is not enough to confer standing. 2013 WL 1282980, at *5.

3. Viacom Has No Liability Under ECPA for Google's Conduct.

There is no aiding and abetting liability under the Wiretap Act. *See, e.g., Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1247 (10th Cir. 2012), *cert. denied*, 133 S. Ct. 2743 (2013) (observing that civil liability provisions “do[] not encompass aiders or abettors”); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 168–69 (5th Cir. 2000) (holding that the “plain language of the statute is unambiguous” that there is no action for procuring). Plaintiffs nevertheless seek to impose secondary liability on Viacom, based on dicta from *Lonegan v. Hasty*, 436 F. Supp. 2d 419 (E.D.N.Y. 2006). Pl. Br. 36–37. There, the court concluded that “changes to [Section 2520] were cosmetic rather than substantive” based on Congressional silence, but also noted that its views were not determinative because plaintiffs had adequately asserted direct interception. *Lonegan*, 436 F. Supp. 2d at 428.

Lonegan's view that the ECPA's 1986 revisions did not eradicate procurement liability has been rejected by the majority of courts that have considered the issue in well-reasoned opinions. In *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, for example, the court rejected *Lonegan* and noted that

the plain language of the statute limits civil liability to interception, disclosure, and use. As one court of appeals has observed, “if Congress did not intend to delete a civil procurement action, it can amend [the statute].” Congress has not done so, even though the interpretation the Court adopts

today [counter to *Lonegan*] has been the clear majority position for well over a decade.

891 F. Supp. 2d 13, 24 (D.D.C. 2012) (quoting *Peavy*, 221 F.3d at 169). *Lonegan* has been classified as the “lone outlier in interpreting the 1986 amendment to [Section] 2520(a)” and its position has been dismissed as dicta. *Shefts v. Petrakis*, 954 F. Supp. 2d 769, 775 (C.D. Ill. 2013).

III. Plaintiffs’ State Law Claims Should Be Dismissed.

Because Plaintiffs’ federal claims against Viacom fail, this Court should decline to exercise supplemental jurisdiction over Plaintiffs’ state law claims. *See* Viacom Br. 32. Further, Plaintiffs’ state-law theories are expressly preempted by federal law and their allegations do not support any state law claim. *Id.* 32–34.

A. COPPA Preempts Plaintiffs’ State Law Claims.

COPPA explicitly states that “[n]o State or local government may impose *any liability* for commercial activities or actions . . . in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.” 15 U.S.C. § 6502(d) (emphasis added). Nothing in COPPA forbids the sort of routine cookie-based data collection and use from minors alleged here, so liability based on Plaintiffs’ state claims would, by definition, require Internet content providers to obtain consents in ways that are inconsistent with COPPA’s detailed statutory and regulatory regime.

In addition to COPPA's express preemption, the Complaint fails because Plaintiffs seek to impose state law liability on Viacom, even though there are no allegations of any COPPA violations. That triggers conflict preemption. Viacom Br. 32–33.

As to the children under 13 who are at issue here, COPPA does not legislate a floor upon which state laws may build additional bases for liability. Viacom Br. 33–34. The *Cohen* decision shows why. *See Cohen v. Facebook, Inc.*, Case No. BC444482 (Cal. Super., minute order Sept. 30, 2011) (opinion attached as appendix to the Memorandum of Law in Support of Viacom Inc.'s Motion to Dismiss). The plaintiffs in *Cohen* unsuccessfully attempted to impose liability where COPPA does not (parental consent for users over the age of 12 where COPPA does not require it); Plaintiffs here attempt to do the same (parental consent for users under the age of 13 where COPPA does not require it). The state-law claims therefore should be dismissed as preempted.

B. Plaintiffs Fail to State a Claim Under State Law.

1. Plaintiffs Have Not Stated a Claim Under the California Invasion of Privacy Act.

A URL is not the contents of a communication. *See supra* Part II.B.2. Plaintiffs thus fail to state a claim under the California Invasion of Privacy Act (“CIPA”). *See Google Cookie*, 2013 WL 5582866, at *5–6. Plaintiffs' only response is that a log of multiple URLs collected in a cookie and linked to a unique

identifier should be considered CIPA-actionable contents. Pl. Br. 43. This argument fails for the reasons described in *Google Cookie*. That decision explicitly based its holding on *United States v. Allen*, in which a “log identifying the date, time, user, and detailed Internet address of sites accessed” was considered a transactional record, and *not* contents. *Google Cookie*, 2013 WL 5582866, at *5 (citing *United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000)).

2. Plaintiffs Have Not Stated a Claim Under the New Jersey Computer Related Offenses Act.

Plaintiffs’ New Jersey Computer Related Offenses Act (“NJCROA”) allegations, in both their Complaint, ¶¶ 189–90, and the NJCROA argument articulated in their brief, Pl. Br. 52, literally offer no more than “a formulaic recitation of the elements of a cause of action.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *see id.* at 564 (“[O]n fair reading these are merely legal conclusions resting on the prior allegations . . .”). In their brief, Plaintiffs again go beyond their own Complaint, adding the allegation that they undertook “an investigation that took time and money to identify and remove the offensive cookie software,” Pl. Br. 53, a required element of an NJCROA claim that is not pled in the Complaint.

The NJCROA clearly was designed to cover situations entirely dissimilar from Plaintiffs’ claims. *See, e.g., PNY Technologies, Inc. v. Salhi*, No. 2:12-cv-04916, 2013 WL 4039030, at *6 (D.N.J. Aug. 5, 2013) (describing allegation that

the defendant exceeded his authorization by destroying data). When enacted, the NJCROA was paired with a criminal provision designed to target “computer abuse,” including hacking and related threats to computer security. No. 1301, A1301, ch. 184, 1984 N.J. Laws 1 (1984). The New Jersey legislature had specific harms in mind when passing the statutes, including police officers misusing official records, the unauthorized tampering of hospital records, the destruction of computer data causing \$25,000 or more in damages, and making illegal bank transfers. *Id.* at 1–2. Consistent with these purposes, the language of the NJCROA sets forth a range of prohibited activities that all amount to computer hacking. *See, e.g.,* N.J. Stat. 2A:38A-3(a) (prohibiting the “unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment”). None of these examples even remotely comes close to Viacom’s actions. Nor is Plaintiffs’ argument that they are minors relevant under the NJCROA, which on its face does not treat adults and minors any differently.

3. Plaintiffs Have Not Stated a Claim for Intrusion Upon Seclusion or Unjust Enrichment.

Plaintiffs make no effort to defend their tort claims under the laws of any State other than New Jersey. Pl. Br. 55–57. That is a concession that they have no position under the laws of the six other states discussed in Viacom’s opening brief. Viacom Br. 35–39.

Viacom also established that New Jersey law does not permit an independent cause of action for unjust enrichment. *See* Viacom Br. 37 (citing *Nat'l Amusements, Inc. v. N.J. Turnpike Auth.*, 261 N.J. Super. 468, 478 (N.J. Super. 1992), *aff'd*, 275 N.J. Super. 134 (N.J. App. Div. 1994) (“Unjust enrichment is not an independent theory of liability, but is the basis for a claim of quasi-contractual liability.”)). Plaintiffs offer no response. Nor do they explain their failure to plead how Viacom’s alleged conduct deprived them of their ability to capitalize on their browsing histories – a necessary element of any claim for unjust enrichment. *See, e.g., Vill. of Bloomingdale v. CDG Enterprises, Inc.*, 196 Ill. 2d 484, 500 (2001) (unjust enrichment requires that the defendant “enrich himself unjustly *at the expense of another*”) (emphasis added); *see also* Viacom Br. 37–38; Pl. Br. 60. Plaintiffs’ unjust enrichment claim has no basis in New Jersey law (or that of any other state) and should be dismissed.

The intrusion upon seclusion claim fails because that tort requires that the alleged action be “highly offensive to a reasonable person.” *G.D. v. Kenny*, 205 N.J. 275, 309 (2011) (internal quotation marks omitted); *see also* Viacom Br. 36. The use of cookies to collect browsing activity tied to an anonymous identifier cannot, as a matter of law, be deemed highly offensive: it has repeatedly been found to be lawful and is widely used by nearly every commercial website. *See Google Cookie*, 2013 WL 5582866, at *5; *DoubleClick*, 154 F. Supp. 2d at 519.

Moreover, the very notion that the operator of a public website “intrudes” upon the “seclusion” of a visitor to the site, simply by collecting anonymous data to support the site’s operations, makes no sense. Plaintiffs’ intrusion upon seclusion claim has no basis in New Jersey law, nor in the law of any other state.

CONCLUSION

This Court should dismiss the Complaint in its entirety and with prejudice.

DATED: April 2, 2014

DEBEVOISE & PLIMPTON LLP

By: /s/ Bruce P. Keller

Stephen M. Orlofsky
BLANK ROME, LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540
(609) 750-7700

Bruce P. Keller
Jeremy Feigelson
(*Pro Hac Vice* admission pending)
Kristin Lieske Bryan
(*Pro Hac Vice* admission pending)
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, NY 10022
(212) 909-6000

Attorneys for Defendant Viacom Inc.